(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平5－35679

(43)公開日　平成５年(1993)２月12日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ｅ	7323－5L		
12/14	３２０　Ｃ	9293－5B		

審査請求　未請求　請求項の数２(全　８　頁)

(21)出願番号　特願平3－186762

(22)出願日　平成３年(1991)７月26日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　依知川　恭世
東京都港区芝五丁目７番１号日本電気株式会社内

(74)代理人　弁理士　内原　晋

(54)【発明の名称】　データ通信方式

(57)【要約】

【構成】ホストコンピュータと複数の端末との間を電話回線で接続し、前記端末の個別利用者が暗号化されたパスワードをデータに付加し前記ホストコンピュータのデータベースに備えられたパスワードテーブルにより解読して通信を行うデータ通信方式において、前記パスワードデータに時間データのメッセージを付加して少なくとも１時間ごとに時間データに対応した変換文字データでパスワードを変換する。

【効果】不正な端末利用者がホスト・コンピュータを使用するのを困難とし、機密保持を確実にできる。

パスワード・メッセージデータ ("Password:")	時間データ (H)

(a)

時間	加減の文字	アスキーコード	時間	加減の文字	アスキーコード
1時	A	41H	13時	M	4DH
2時	B	42H	14時	N	4EH
3時	C	43H	15時	O	4FH
4時	D	44H	16時	P	50H
5時	E	45H	17時	Q	51H
6時	F	46H	18時	R	52H
7時	G	47H	19時	S	53H
8時	H	48H	20時	T	54H
9時	I	49H	21時	U	55H
10時	J	4AH	22時	V	56H
11時	K	4BH	23時	W	57H
12時	L	4CH	24時	X	58H

(b)

1

【特許請求の範囲】

【請求項１】　ホストコンピュータと複数の端末との間を電話回線で接続し、前記端末の個別利用者がパスワードを入力し前記ホストコンピュータのデータベースに備えられたパスワードテーブルにより解読して通信を行うデータ通信方式において、前記パスワードデータに時間データのメッセージを付加して少なくとも１時間ごとに時間データに対応した変換文字データでパスワードを変換することを特徴とするデータ通信方式。

【請求項２】　ホストコンピュータのデータベースに記憶された前記変換文字データの更新を端末側利用者により自由に更新する手段を備えていることを特徴とする請求項１記載のデータ通信方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はデータ通信方式に関し、特に情報の機密保持のためにパスワードを時間ごとに変換させてホストコンピュータと端末間のデータの授受を行うデータ通信方式に関する。

【０００２】

【従来の技術】従来、この種のデータ通信方式は、図５に示すようにデータベース１を備えたホストコンピュータ２と複数の端末３，４との間で電話回線を介してデータの授受を行うが、データベース１は端末の利用者個別のパスワードテーブルを記憶している。したがって端末からパスワードを入力すると、パスワードに対しての暗号化がなされ、ホストコンピュータ２が、パスワードの照合を行うことによって、端末からパスワードを入力した利用者は、アクセス権を得ることが出来る。ここでパスワードに対しての暗号化は、固定でおこなわれていた。

【０００３】

【発明が解決しようとする課題】上述した従来の固定されたパスワード変換データ通信の方法では、不正使用者のパスワード解読が容易であり、情報の機密保持が著しく損なわれる欠点があった。

【０００４】本発明の目的は、パスワードに対する暗号化が、従来の様に固定でなく、時間とともに変化させることが可能であること、又、端末の利用者が、時間とともに使用される変換文字を書換えることが可能であることにより、不正使用者に対する情報の機密保持をはかることにある。

【０００５】

【課題を解決するための手段】本発明のデータ通信方式は、ホストコンピュータと複数の端末との間を電話回線で接続し、前記端末の個別利用者がパスワードを入力し前記ホストコンピュータのデータベースに備えられたパスワードテーブルにより解読して通信を行うデータ通信方式において、前記パスワードデータに時間データのメッセージを付加して少なくとも１時間ごとに時間データ

2

に対応した変換文字データでパスワードを変換する。

【０００６】

【実施例】次に本発明について図面を参照して説明する。図１（ａ），（ｂ）は本発明の一実施例のデータフォーマットおよび時間データのコードの説明図、図２は本実施例の端末側の動作を示すフローチャート、図３はホストコンピュータ側の動作を示すフローチャート、図４は本実施例の端末側においてパスワードの文字を変換する場合のフローチャートである。まず、図１（ａ）のデータフォーマットにおいて、利用者個別のパスワードとメッセージに新たに時間データを付加している。したがって一時間経過するごとにパスワードを変えてデータの秘とく性を高くしている。図１（ｂ）は時間データのフォーマットの一例であり、１時から１時間ごとに２４時までのコードを表のように変換方法における変換文字が入っているとすると、まず、時間情報が１Ｈ（Ｈｏｕｒ）のとき、暗号化されたパスワードのデータの１文字ずつに、Ａのアスキーコード（４１Ｈ）の下５ビットを加えていってデータを変換する。そのとき、１文字８ビットであり１文字ごとに下５ビットに同じデータ変換を行う。同じように、図１（ｂ）の表が示しているコードを時間によって変えて変換を行う。そしてデータをホスト・コンピュータに送る。

【０００７】次に端末側のパスワード授受のフローチャートを図２により説明する。端末の使用者がログインして（Ｓ１）、ホストコンピュータからのメッセージＢに時間の情報が付加されているので、まずその時間の情報を、送信するパスワードに付加して一緒に送る。そして送られる暗号化されたパスワードのデータをバッファに格納する（Ｓ２～Ｓ４）。今度は、バッファからパスワードに付加された時間の情報を読み込んでくる（Ｓ５）。そして、時間ごとに変換方法が決っているので、送られてきた暗号化されたパスワードのデータを変換する（Ｓ６～Ｓ１１）。そして、変換されたパスワードＣをホスト・コンピュータに送信する（Ｓ１２）。変換方法に利用する変換文字は、後述するように端末の利用者が変換することが可能である。

【０００８】次に、ホストコンピュータ側の動作のフローチャートを図３により説明する。まず、ホスト・コンピュータ側では端末にパスワードを要求し（ＳＩＡ）、端末側からの暗号化されたパスワードのデータを変換したデータが送られてくるので、送られてきたデータをバッファに入力する（Ｓ３Ａ）。そして、データに付加している時間の情報を読み込む（Ｓ４Ａ）。時間の情報によって、変換されたデータをもとのパスワードに復号化する変換を行う（Ｓ５Ａ～Ｓ１０Ａ）。そして、ホスト・コンピュータは、パスワードの照合を行う（Ｓ１１Ａ）。例えば、時間情報が１Ｈ（Ｈｏｕｒ）のとき、端末側で変換されたデータを、もとにパスワードに復号化するために、端末で行われた処理と反対の処理を行うた

めに、データの１文字ずつに、Ａのアスキーコード（４１Ｈ）の下５ビットを引いていってデータを変換する。そのとき、１文字８ビットであり１文字ごとに下５ビットに、同じデータ変換を行う。同じように、図１（ｂ）の表が示しているコードを時間によって変えて変換を行う。このように、暗号化されたパスワードのデータがもとの状態に復号化されたことにより、ホスト・コンピュータは、パスワードの照合を行うことが出来る。そして、端末の利用者にアクセス権を与えることが出来る（図２のＳ１３）。

【０００９】次に、端末側でパスワード変換文字更新を行うフローチャートを図４により説明する。端末の利用者が、変換方法に利用する変換文字を更新するときには、ホスト・コンピュータのデータ・ベースから、変換文字が入っているデータ変換テーブルを読み込む（Ｓ２１）。そしてデータ変換テーブルのデータを更新する（Ｓ２３）。更新されたデータ変換テーブルと同じものが、端末側のファイルにも存在するので、端末側の変換文字が入っているデータ変換テーブルを更新する（Ｓ２４）。なお、パスワードの文字列においては、１文字８ビットであり１文字ごとの下５ビットに、時間に対する変換文字の下５ビットを１文字ずつ所定の計算（加減算）する変換を行う。データ変換のときに利用される変換文字は、端末の利用者が変換可能であり、よりいっそうの情報の機密保持を計っている。

【００１０】

【発明の効果】以上説明したように本発明はパスワードを時々刻々変更し、かつ端末利用者のみがホスト・コンピュータの記憶媒体内のデータ変換テーブルを自由に更新できる様にしたことにより、不正な端末利用者がホスト・コンピュータを使用するのを困難とし、機密保持を確実にできる効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例のデータフォーマット図（ａ）、および時間データのコードを示す説明図（ｂ）である。

【図２】本実施例の端末側のフローチャートである。

【図３】本実施例のホストコンピュータ側のフローチャートである。

【図４】本実施例の端末側の変換文字更新のフローチャートである。

【図５】一般的なデータ通信システムの構成図である。

【符号の説明】

１　　データベース

２　　ホストコンピュータ

３，４　　端末

Ｓ１～Ｓ１３　　端末側のフローチャートのステップ

Ｓ１Ａ～Ｓ１１Ａ　　ホストコンピュータ側のフローチャートのステップ

Ｓ２１～Ｓ２４　　端末側の変換文字更新のフローチャートのステップ

【図１】

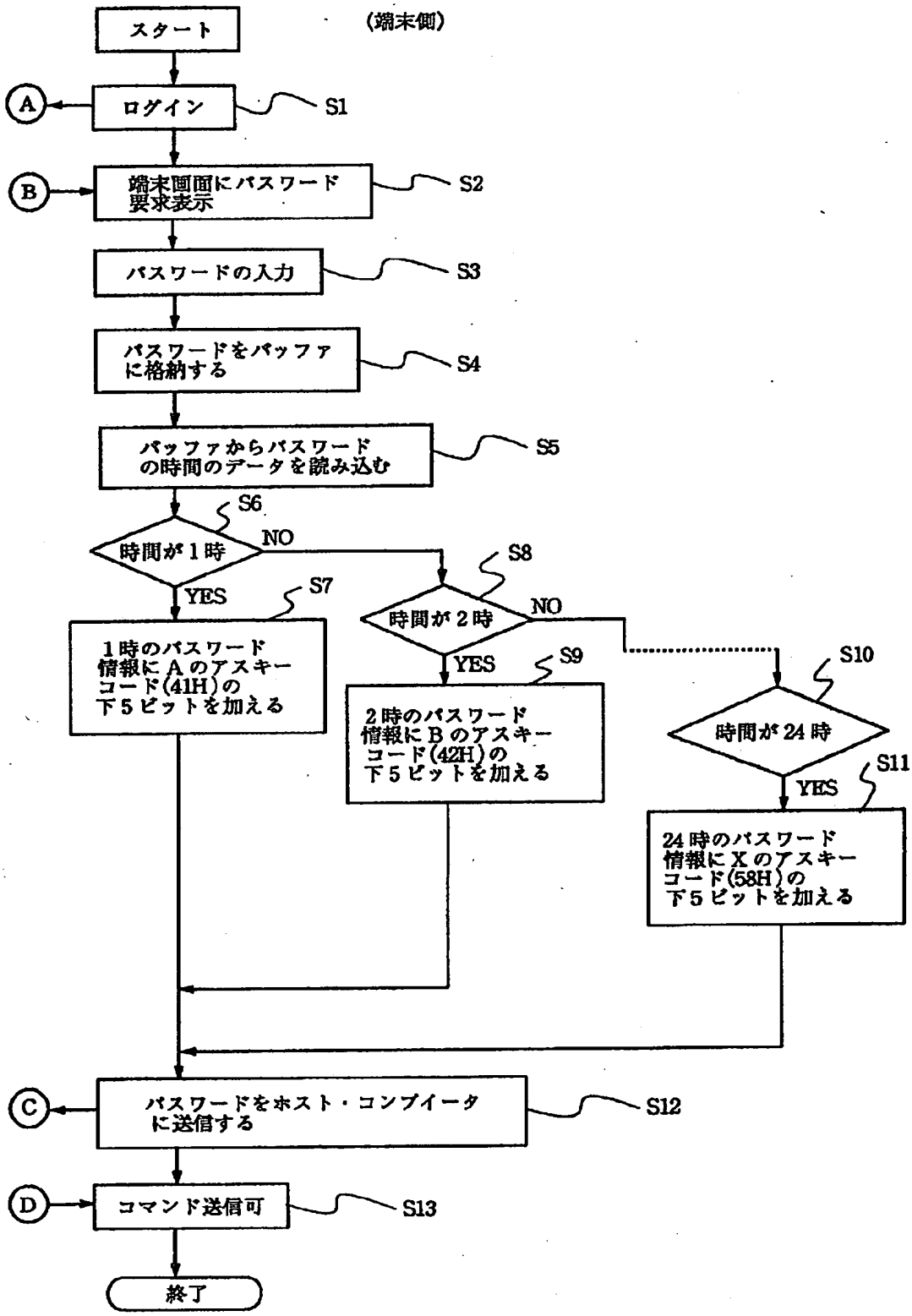
パスワード・メッセージデータ ("Password:")	時間データ (H)

(a)

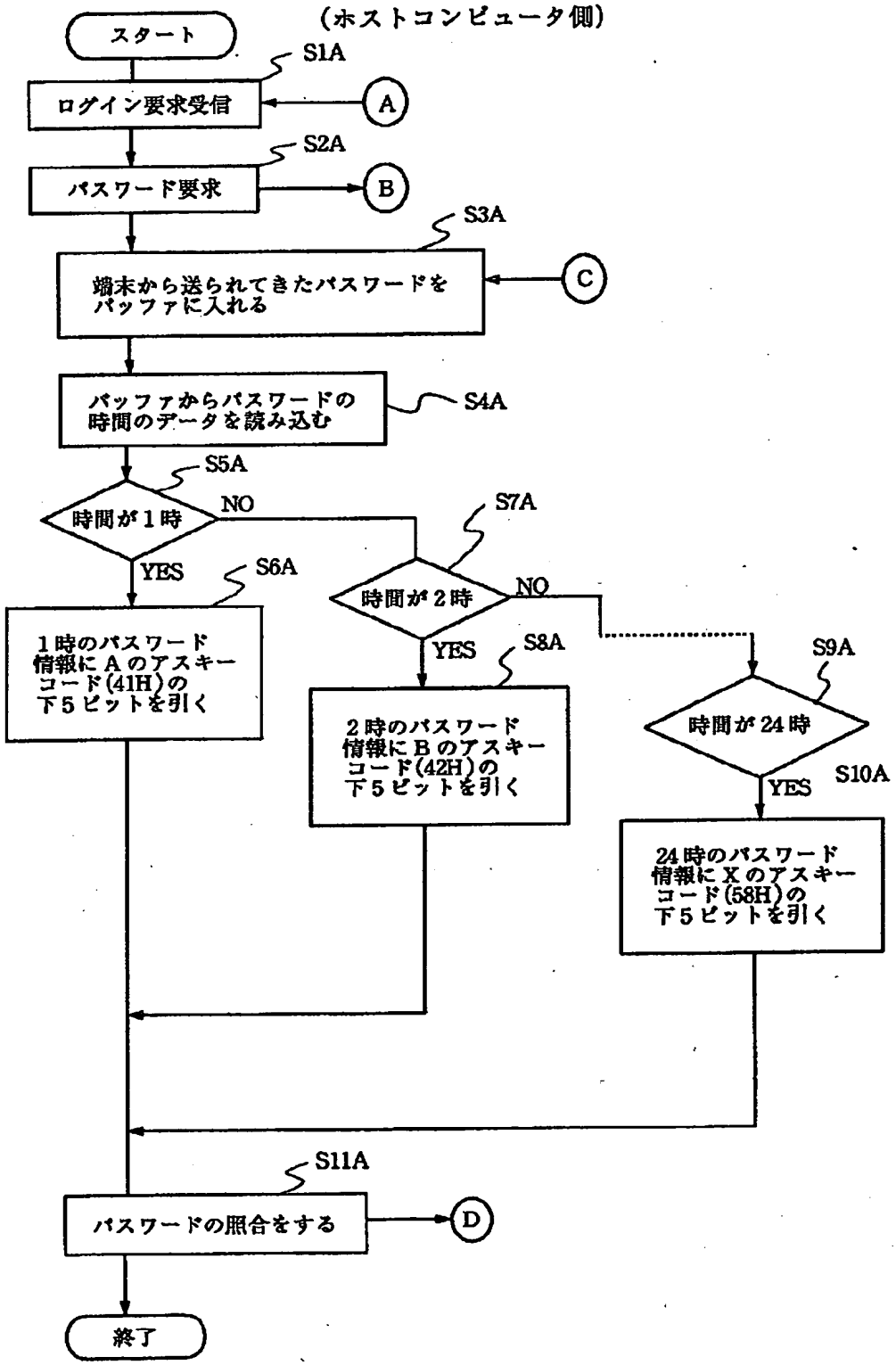
時間	加減の文字	アスキーコード	時間	加減の文字	アスキーコード
1時	A	41H	13時	M	4DH
2時	B	42H	14時	N	4EH
3時	C	43H	15時	O	4FH
4時	D	44H	16時	P	50H
5時	E	45H	17時	Q	51H
6時	F	46H	18時	R	52H
7時	G	47H	19時	S	53H
8時	H	48H	20時	T	54H
9時	I	49H	21時	U	55H
10時	J	4AH	22時	V	56H
11時	K	4BH	23時	W	57H
12時	L	4CH	24時	X	58H

(b)

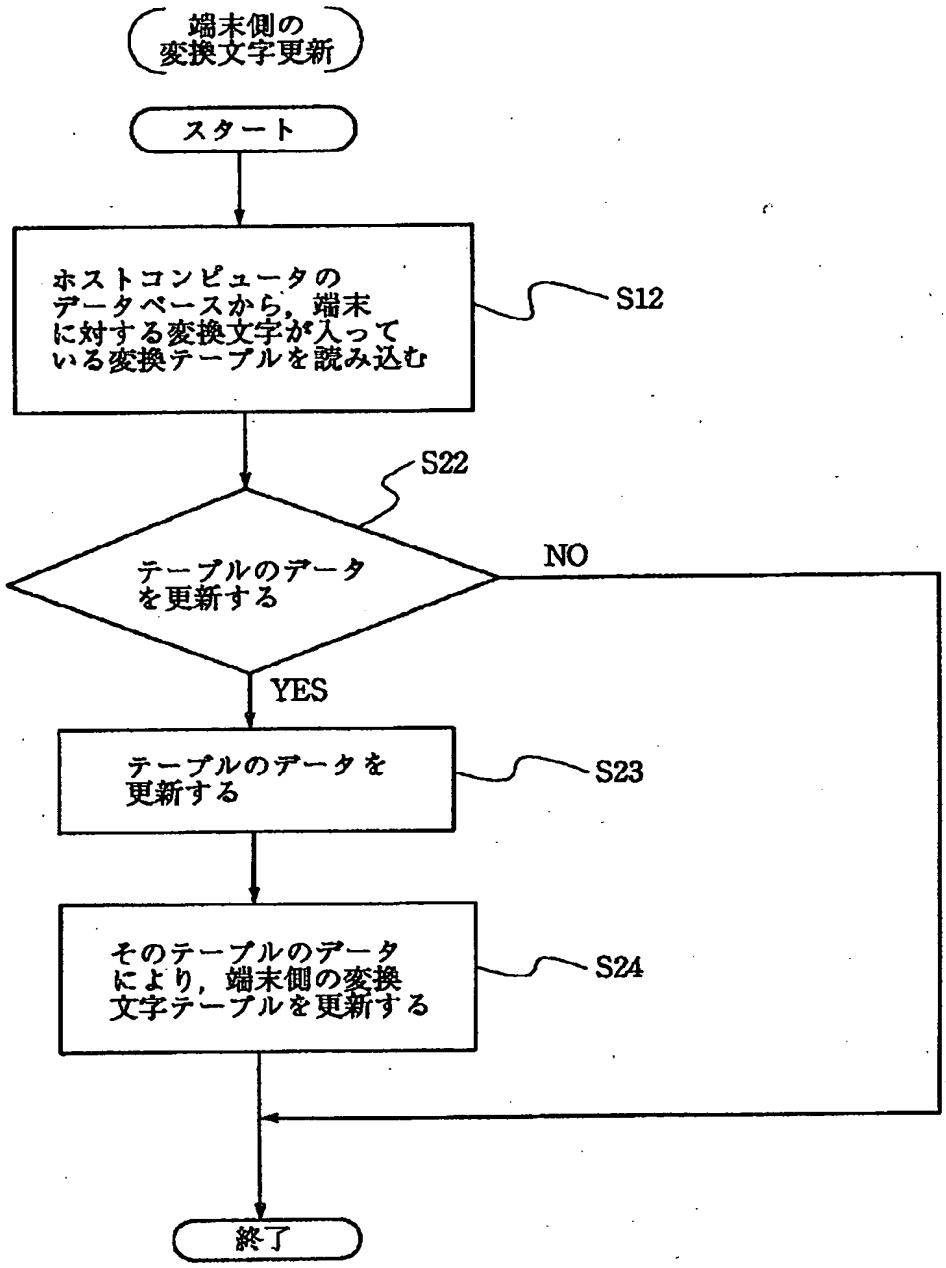
【図２】


スタート
(端末側)
A
ログイン
S1
B
端末画面にパスワード要求表示
S2
パスワードの入力
S3
パスワードをバッファに格納する
S4
バッファからパスワードの時間のデータを読み込む
S5
S6
時間が１時
NO
YES
S7
１時のパスワード情報にＡのアスキーコード(41H)の下５ビットを加える
S8
時間が２時
NO
YES
S9
２時のパスワード情報にＢのアスキーコード(42H)の下５ビットを加える
S10
時間が24時
YES
S11
24時のパスワード情報にＸのアスキーコード(58H)の下５ビットを加える
C
パスワードをホスト・コンピュータに送信する
S12
D
コマンド送信可
S13
終了

【図３】


(ホストコンピュータ側)
スタート
S1A
ログイン要求受信
A
S2A
パスワード要求
B
S3A
端末から送られてきたパスワードを
バッファに入れる
C
バッファからパスワードの
時間のデータを読み込む
S4A
S5A
時間が１時
NO
S7A
YES
S6A
時間が２時
NO
１時のパスワード
情報にＡのアスキー
コード(41H)の
下５ビットを引く
YES
S8A
S9A
２時のパスワード
情報にＢのアスキー
コード(42H)の
下５ビットを引く
時間が24時
S10A
YES
24時のパスワード
情報にＸのアスキー
コード(58H)の
下５ビットを引く
S11A
パスワードの照合をする
D
終了

【図４】


端末側の
変換文字更新
スタート
ホストコンピュータの
データベースから，端末
に対する変換文字が入って
いる変換テーブルを読み込む
S12
S22
テーブルのデータ
を更新する
NO
YES
テーブルのデータを
更新する
S23
そのテーブルのデータ
により，端末側の変換
文字テーブルを更新する
S24
終了

【図５】